U.S. Patent Application Serial No. 09/869,966

Claims as Filed in Amendment dated August 17, 2006

Listing of Claims:

1-12. (Cancelled)

13. (Currently Amended) A system for producing asymmetric cryptographic keys, said keys comprising $m \geq 1$ private values $Q_1, Q_2, ..., Q_m$ and m respective public values $G_1, G_2, ..., G_m$, the system comprising:

a processor; and

a memory unit coupled to the processor, the memory unit storing a set of instructions which when executed cause the processor to execute the following acts:

selecting a security parameter k, wherein k is an integer greater than 1;

~~selecting m base numbers $g_1, g_2, ..., g_m$, wherein each base number g_i (for $i = 1, ..., m$) is an integer greater than 1;~~

determining a modulus n, wherein n is a public integer equal to the product of at least two prime factors $p_1, ..., p_f$, at least two of these prime factors, say p_1 and p_2, being such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$;

selecting m base numbers $g_1, g_2, ..., g_m$, wherein each base number g_i (for $i = 1, ..., m$) is an integer greater than 1 and is a non-quadratic residue of the ring of integers modulo n, and such that p_2 is complementary to p_1 with respect to one of the base numbers;

calculating the public values G_i for $i = 1, ..., m$ through $G_i \equiv g_i^2 \bmod n$; and

calculating the private values Q_i for $i = 1,...,m$ by solving either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein the public exponent v is such that $v = 2^k$.

14. (Previously presented) The system according to claim 13, wherein the number $(f-e)$ (where $e \geq 0$) of prime factors of the modulus n which are congruent to 3 mod 4 is larger than 2, and those prime factors p_{j+1} for $2 \leq j \leq m$ which are congruent to 3 mod 4 are determined iteratively as follows:

the profile $\text{profile}_j(g_j)$ of g_j with respect to the prime factors $p_1, p_2,..., p_j$ is computed, and

if $\text{profile}_j(g_j)$ is flat, then the prime factor p_{j+1} is chosen such that p_{j+1} is complementary to p_1 with respect to g_j; else, a number g is chosen among the $(j-1)$ base numbers $g_1, g_2,..., g_{j-1}$ and all of their multiplicative combinations, such that $\text{profile}_j(g) = \text{profile}_j(g_j)$, then p_{j+1} is chosen such that $\text{profile}_{j+1}(g_j) \neq \text{profile}_{j+1}(g)$,

wherein the last prime factor p_{f-e} congruent to 3 mod 4 is, in the case that $f-e \leq m$, chosen such that p_{f-e} is complementary to p_1 with respect to all of the base numbers g_i such that $f-e \leq i \leq m$ and whose profile $\text{profile}_{f-e-1}(g_i)$ is flat.

15. (Previously Presented) The system according to claim 13, wherein the number e of prime factors of the modulus n which are congruent to 1 mod 4 is at least equal to 1, and each such prime factor is determined as follows:

a candidate prime number p is chosen, such that the Legendre symbol of each base number g_i (for $i = 1,...,m$) with respect to p is equal to $+1$,

the integer t is computed which is such that $(p-1)$ is divisible by 2^t, but not by 2^{t+1},

the integer $s=(p-1+2^t)/2^{t+1}$ is computed,

an integer $b \equiv h^{p-1/2^t} \bmod p$, where h is a non-quadratic residue of the body of integers modulo p, is computed,

the m integers $r_i \equiv g_i^{2s} \bmod p$ for $i = 1,...,m$ are computed,

an integer u is initialized to $u = 0$,

the following sequence of steps, where i is initialized to 1, is iteratively implemented:

an integer w is initialized to $w = r_i$,

if $r_i = \pm g_i$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i < m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i = m$,

if $r_i \neq \pm g_i$:

an integer jj is initialized to 1,

the following sequence of steps, where an integer ii is initialized to 1, is iteratively implemented :

$x \equiv w^2 / g_i^2 \bmod p$ is computed,

$y \equiv x^{2^{t-ii-1}} \bmod p$ is computed, and

if $y = +1$, the sequence is terminated at the current value of ii,

if $y=-1$, jj is assigned the value $jj=2^{ii}$, the number w is assigned a new value equal to the old value multiplied by b^{jj} modulo p, and

for $ii<t-2$, the value of ii is incremented and a new iteration is proceeded to with the new value of ii,

for $ii=t-2$, the value of number u is updated through the relation $jj=2^{t-u}$, and

if $t-u<k$, the candidate prime number p is rejected as a factor of the modulus n,

if $t-u>k$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i<m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i=m$.

16. (Previously presented) The system according to claim 15, wherein, to compute the $f \cdot m$ private components $Q_{i,j}$ of the private values $Q_1, Q_2, \ldots, Q_m$, the following steps are implemented for each couple (i,j):

an integer t is determined, which is equal to 1 if p_j is congruent to 3 mod 4, and to the value obtained for t according to claim 15 if p_j is congruent to 1 mod 4,

an integer u is determined, which is equal to 0 if p_j is congruent to 3 mod 4, and to the value obtained for u according to claim 15 if p_j is congruent to 1 mod 4,

the integer $z \equiv G_i^s \bmod p_j$ is computed, where $s=(p-1+2^t)/2^{t+1}$,

all the numbers zz are being considered, which:

if $u = 0$, are such that $zz = z$ or such that zz is equal to the product modulo p_j of z by each of the 2^{ii-1} 2^{ii}-th primitive roots of unity, for ii ranging from 1 to $\min(k,t)$,

if $u > 0$, are such that zz is equal to the product modulo p_j of za by each of the 2^k 2^k-th roots of unity, where za is the value obtained for w according to claim 15, and

for each such number zz, a value for the component $Q_{i,j}$ is obtained by taking $Q_{i,j}$ equal to zz if the equation $G_i \equiv Q_i^v \bmod n$ is used, or to the inverse of zz modulo p_j if $G_i \cdot Q_i^v \equiv 1 \bmod n$ is used for this value of i.

17. (Currently Amended) A computer-readable storage medium storing instructions for producing asymmetric cryptographic keys, said keys comprising $m \geq 1$ private values $Q_1, Q_2, \ldots, Q_m$ and m respective public values $G_1, G_2, \ldots, G_m$, the medium storing instructions which when executed cause a processor to execute the following acts:

selecting a security parameter k, wherein k is an integer greater than 1;

~~selecting m base numbers $g_1, g_2, \ldots, g_m$, wherein each base number g_i (for $i = 1, \ldots, m$) is an integer greater than 1;~~

determining a modulus n, wherein n is a public integer equal to the product of at least two prime factors $p_1, \ldots, p_f$, at least two of these prime factors, say p_1 and p_2, being such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$;

selecting m base numbers $g_1, g_2, \ldots, g_m$, wherein each base number g_i (for $i = 1, \ldots, m$) is an integer greater than 1 and is a non-quadratic residue of the ring of integers modulo n, and such that p_2 is complementary to p_1 with respect to one of the base numbers;

calculating the public values G_i for $i = 1, \ldots, m$ through $G_i \equiv g_i^{\,2} \bmod n$; and

calculating the private values Q_i for $i = 1, \ldots, m$ by solving either the equation $G_i \cdot Q_i^{\,v} \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^{\,v} \bmod n$, wherein the public exponent v is such that $v = 2^k$.

18. (Previously presented) The computer-readable storage medium storing instructions according to claim 17, wherein the number $(f - e)$ (where $e \geq 0$) of prime factors of the modulus n which are congruent to 3 mod 4 is larger than 2, and those prime factors p_{j+1} for $2 \leq j \leq m$ which are congruent to 3 mod 4 are determined iteratively as follows:

the profile $\text{profile}_j(g_j)$ of g_j with respect to the prime factors $p_1, p_2, \ldots, p_j$ is computed, and

if $\text{profile}_j(g_j)$ is flat, then the prime factor p_{j+1} is chosen such that p_{j+1} is complementary to p_1 with respect to g_j; else, a number g is chosen among the $(j-1)$ base numbers $g_1, g_2, \ldots, g_{j-1}$ and all of their multiplicative combinations, such that $\text{profile}_j(g) = \text{profile}_j(g_j)$, then p_{j+1} is chosen such that $\text{profile}_{j+1}(g_j) \neq \text{profile}_{j+1}(g)$,

wherein the last prime factor p_{f-e} congruent to 3 mod 4 is, in the case that $f - e \leq m$, chosen such that p_{f-e} is complementary to p_1 with respect to all of the base numbers g_i such that $f - e \leq i \leq m$ and whose profile $\text{profile}_{f-e-1}(g_i)$ is flat.

19. (Previously presented) The computer-readable storage medium storing instructions according to claim 17, wherein the number e of prime factors of the modulus n which are congruent to 1 mod 4 is at least equal to 1, and each such prime factor is determined as follows:

a candidate prime number p is chosen, such that the Legendre symbol of each base number g_i (for $i = 1,...,m$) with respect to p is equal to $+1$,

the integer t is computed which is such that $(p-1)$ is divisible by 2^t, but not by 2^{t+1},

the integer $s = (p-1+2^t)/2^{t+1}$ is computed,

an integer $b \equiv h^{p-1/2^t} \bmod p$, where h is a non-quadratic residue of the body of integers modulo p, is computed,

the m integers $r_i \equiv g_i^{2s} \bmod p$ for $i = 1,...,m$ are computed,

an integer u is initialized to $u = 0$,

the following sequence of steps, where i is initialized to 1, is iteratively implemented:

an integer w is initialized to $w = r_i$,

if $r_i = \pm g_i$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i < m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i = m$,

if $r_i \neq \pm g_i$:

an integer jj is initialized to 1,

the following sequence of steps, where an integer ii is initialized to 1, is iteratively implemented :

$x \equiv w^2 / g_i^2 \bmod p$ is computed,

$y \equiv x^{2^{t-ii-1}} \bmod p$ is computed, and

if $y = +1$, the sequence is terminated at the current value of ii,

if $y = -1$, jj is assigned the value $jj = 2^{ii}$, the number w is assigned a new value equal to the old value multiplied by b^{jj} modulo p, and

for $ii < t-2$, the value of ii is incremented and a new iteration is proceeded to with the new value of ii,

for $ii = t-2$, the value of number u is updated through the relation $jj = 2^{t-u}$, and

if $t-u < k$, the candidate prime number p is rejected as a factor of the modulus n,

if $t-u > k$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i < m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i = m$.

20. (Previously Presented) The computer-readable storage medium storing instructions according to claim 19, wherein, to compute the $f \cdot m$ private components $Q_{i,j}$ of the private values $Q_1, Q_2, \ldots, Q_m$, the following steps are implemented for each couple (i, j):

an integer t is determined, which is equal to 1 if p_j is congruent to 3 mod 4, and to the value obtained for t according to claim 19 if p_j is congruent to 1 mod 4,

an integer u is determined, which is equal to 0 if p_j is congruent to 3 mod 4, and to the value obtained for u according to claim 19 if p_j is congruent to 1 mod 4,

the integer $z \equiv G_i^s \bmod p_j$ is computed, where $s = (p - 1 + 2^t)/2^{t+1}$,

all the numbers zz are being considered, which:

> if $u = 0$, are such that $zz = z$ or such that zz is equal to the product modulo p_j of z by each of the 2^{ii-1} 2^{ii}-th primitive roots of unity, for ii ranging from 1 to $\min(k,t)$,
>
> if $u > 0$, are such that zz is equal to the product modulo p_j of za by each of the 2^k 2^k-th roots of unity, where za is the value obtained for w according to claim 19, and

for each such number zz, a value for the component $Q_{i,j}$ is obtained by taking $Q_{i,j}$ equal to zz if the equation $G_i \equiv Q_i^v \bmod n$ is used, or to the inverse of zz modulo p_j if $G_i \cdot Q_i^v \equiv 1 \bmod n$ is used for this value of i.

21. (Currently Amended) A computer-implemented process for producing asymmetric cryptographic keys, said keys comprising $m \geq 1$ private values $Q_1, Q_2, \ldots, Q_m$ and m respective public values $G_1, G_2, \ldots, G_m$, the computer-implemented process comprising:

selecting a security parameter k, wherein k is an integer greater than 1;

~~selecting m base numbers $g_1, g_2, \ldots, g_m$, wherein each base number g_i (for $i = 1, \ldots, m$) is an integer greater than 1;~~

determining a modulus n, wherein n is a public integer equal to the product of at least two prime factors $p_1, \ldots, p_f$, at least two of these prime factors, say p_1 and p_2, being such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$;

<u>selecting m base numbers $g_1, g_2, \ldots, g_m$, wherein each base number g_i (for $i = 1, \ldots, m$) is an integer greater than 1 and is a non-quadratic residue of the ring of integers modulo n</u>, and such that p_2 is complementary to p_1 with respect to one of the base numbers;

calculating the public values G_i for $i = 1, \ldots, m$ through $G_i \equiv g_i^2 \bmod n$; and

calculating the private values Q_i for $i = 1, \ldots, m$ by solving either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein the public exponent v is such that $v = 2^k$.

22. (Previously Presented) The computer-implemented process according to claim 21, wherein the number $(f - e)$ (where $e \geq 0$) of prime factors of the modulus n which are congruent to 3 mod 4 is larger than 2, and those prime factors p_{j+1} for $2 \leq j \leq m$ which are congruent to 3 mod 4 are determined iteratively as follows:

the profile $\text{profile}_j(g_j)$ of g_j with respect to the prime factors $p_1, p_2, \ldots, p_j$ is computed, and

if $\text{profile}_j(g_j)$ is flat, then the prime factor p_{j+1} is chosen such that p_{j+1} is complementary to p_1 with respect to g_j; else, a number g is chosen among the $(j-1)$ base

numbers $g_1, g_2, \ldots, g_{j-1}$ and all of their multiplicative combinations, such that $\text{profile}_j(g) = \text{profile}_j(g_j)$, then p_{j+1} is chosen such that $\text{profile}_{j+1}(g_j) \neq \text{profile}_{j+1}(g)$,

wherein the last prime factor p_{f-e} congruent to 3 mod 4 is, in the case that $f - e \leq m$, chosen such that p_{f-e} is complementary to p_1 with respect to all of the base numbers g_i such that $f - e \leq i \leq m$ and whose profile $\text{profile}_{f-e-1}(g_i)$ is flat.

23. (Previously Presented) The computer-implemented process according to claim 21, wherein the number e of prime factors of the modulus n which are congruent to 1 mod 4 is at least equal to 1, and each such prime factor is determined as follows:

a candidate prime number p is chosen, such that the Legendre symbol of each base number g_i (for $i = 1, \ldots, m$) with respect to p is equal to $+1$,

the integer t is computed which is such that $(p-1)$ is divisible by 2^t, but not by 2^{t+1},

the integer $s = (p - 1 + 2^t)/2^{t+1}$ is computed,

an integer $b \equiv h^{p-1/2^t} \bmod p$, where h is a non-quadratic residue of the body of integers modulo p, is computed,

the m integers $r_i \equiv g_i^{2s} \bmod p$ for $i = 1, \ldots, m$ are computed,

an integer u is initialized to $u = 0$,

the following sequence of steps, where i is initialized to 1, is iteratively implemented:

an integer w is initialized to $w = r_i$,

if $r_i = \pm g_i$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i < m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i = m$,

if $r_i \neq \pm g_i$:

an integer jj is initialized to 1,

the following sequence of steps, where an integer ii is initialized to 1, is iteratively implemented :

$x \equiv w^2 / g_i^2 \bmod p$ is computed,

$y \equiv x^{2^{t-ii-1}} \bmod p$ is computed, and

if $y = +1$, the sequence is terminated at the current value of ii,

if $y = -1$, jj is assigned the value $jj = 2^{ii}$, the number w is assigned a new value equal to the old value multiplied by b^{jj} modulo p, and

for $ii < t-2$, the value of ii is incremented and a new iteration is proceeded to with the new value of ii,

for $ii = t-2$, the value of number u is updated through the relation $jj = 2^{t-u}$, and

if $t-u < k$, the candidate prime number p is rejected as a factor of the modulus n,

if $t-u>k$, the value of i is incremented and a sequence of steps with the new value of i is proceeded to if $i<m$, whereas the candidate prime number p is accepted as a factor of the modulus n if $i=m$.

24. (Previously Presented) The computer-implemented process according to claim 23, wherein, to compute the $f \cdot m$ private components $Q_{i,j}$ of the private values $Q_1, Q_2, \ldots, Q_m$, the following steps are implemented for each couple (i, j):

an integer t is determined, which is equal to 1 if p_j is congruent to 3 mod 4, and to the value obtained for t according to claim 23 if p_j is congruent to 1 mod 4,

an integer u is determined, which is equal to 0 if p_j is congruent to 3 mod 4, and to the value obtained for u according to claim 23 if p_j is congruent to 1 mod 4,

the integer $z \equiv G_i^{\,s} \bmod p_j$ is computed, where $s=(p-1+2^t)/2^{t+1}$,

all the numbers zz are being considered, which:

if $u=0$, are such that $zz=z$ or such that zz is equal to the product modulo p_j of z by each of the 2^{ii-1} 2^{ii}-th primitive roots of unity, for ii ranging from 1 to $\min(k,t)$,

if $u>0$, are such that zz is equal to the product modulo p_j of za by each of the 2^k 2^k-th roots of unity, where za is the value obtained for w according to claim 23, and

for each such number zz, a value for the component $Q_{i,j}$ is obtained by taking $Q_{i,j}$ equal to zz if the equation $G_i \equiv Q_i^v \bmod n$ is used, or to the inverse of zz modulo p_j if $G_i \cdot Q_i^v \equiv 1 \bmod n$ is used for this value of i.